

[First response computer virus blocking]

Abstract

A process of screening one or more software files to determine any that are recognized to have a matching hash signature with a file contained in a database of files known to be Virus, Trojan, Worm, or otherwise potentially malicious or suspicious which then can be safely blocked, quarantined and/or deleted. This is accomplished through a method and apparatus running on a firewall, network device, mail server, server, personal computer, PDA, cell phone or wireless device to compare the hash signature of each incoming software file against a regularly updated database of known infected file hash signatures. One or more users can be alerted when an infected file is identified. If quarantined the file is safely stored until virus software is updated properly with later developed virus definitions file(s), which are then used to eradicate or clean the infected file(s) or computer systems.